

- Cont*
- c) acquiring an encryption key value;
 - d) encrypting the file using the encryption key value to create an encrypted file;
 - e) completing the change document command by performing the change document

command upon the encrypted file instead of the file; and

- f) invoking an option to initiate a virus scan program;

wherein steps c) and d) further comprise the steps of:

selecting an algorithm to use with the file from one of a plurality of encryption

algorithms;

selecting an encryption key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;

adding the file identifier to the file; and

using the key value and the selected algorithm to encrypt the file.

48. The method as recited in claim 47, comprising the further step of running a virus scan program on the file before it is encrypted.

49. The method as recited in claim 47, comprising the further steps of selecting the file from within the contents of a second file that is larger than the file.

50. The method as recited in claim 49, comprising the further steps of creating a third file from the second file wherein the third file contains the encrypted file and the portion of the second file that does not include the file.

51. The method as recited in claim 50, wherein the encrypted file is located in a container.

52. The method as recited in claim 47, wherein the algorithm is selected from the plurality of algorithms according to a pre-selected criteria.

53. The method as recited in claim 47, wherein the algorithm is selected from the plurality of algorithms according to a pre-selected algorithm.

54. The method as recited in claim 47, wherein the file identifier is inserted into the file according to a pre-selected criteria.

55. The method as recited in claim 47, wherein the file identifier is inserted into the file according to a pre-selected algorithm.

56. The method as recited in claim 47, wherein there are plural encryption key values and at least one encryption key value is associated with the user.

57. The method as recited in claim 56, comprising the further steps of:

requiring the user to submit to an access authentication step; and

if the access authentication step does not authenticate the user, then skipping steps c) and d), but if the access authentication step does authenticate the user, then retrieving the encryption key value associated with the encryption key name and the user.

58. A method of decrypting an electronic file that is to be opened in an application program running in a suitable environment for operating the program, comprising the steps of:

- a) issuing an open document command to act upon the file;
- b) intercepting the open document command;
- c) retrieving a decryption key value;
- d) decrypting the file using the decryption key value to create an unencrypted file;

and

- e) completing the open document command by performing the open document command upon the unencrypted file instead of the file; and

wherein steps c) and d) further comprise the steps of:

selecting an algorithm to use with the file from one of a plurality of algorithms;

selecting an encryption key with a key value;

inputting a decryption key with a key value;

validating the decryption key value with the key value associated with a file identifier;

using the key value and the selected algorithm to decrypt the file; and

invoking an option to initiate a virus scan program.

59. A method of decrypting an electronic file that is to be opened in an application program running in a suitable environment for operating the program, comprising the steps of:

- a) issuing an open document command to act upon the file;
- b) intercepting the open document command;
- c) retrieving a decryption key value;
- d) decrypting the file using the decryption key value to create an unencrypted file;

and

e) completing the open document command by performing the open document command upon the unencrypted file instead of the file; and
wherein steps c) and d) further comprise the steps of:
selecting an algorithm to use with the file from one of a plurality of algorithms;
inputting a decryption key with a key value;
validating the decryption key value with the key value associated with a file identifier;
using the key value and the selected algorithm to decrypt the file; and
running a virus scan program on the decrypted file.

60. A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;
selecting an encryption key with a key value;
generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;
adding the file identifier to the file;
using the key value and the selected algorithm to encrypt the file and generate an encrypted file;
uniquely identifying the encrypted file with an encrypted data identifier during encryption;
inputting a decryption key with a decryption key value;
validating the decryption key value with the key value associated with the file identifier;

using the key value and the selected algorithm to decrypt the file; and

testing the encrypted data identifier after decryption by regenerating the encrypted data

identifier and ascertaining that they are the same.

61. The method as recited in claim 60, comprising the further step of selecting the file from within the contents of a second file that is larger than the file.

62. The method as recited in claim 61, wherein the encrypted file is placed in a container.

63. The method as recited in claim 62, comprising the further step of creating a third file from the second file wherein the third file contains the encrypted file and the portion of the second file that does not include the file.


64. The method as recited in claim 63, wherein the container is represented in the third file.

65. The method as recited in claim 64, wherein the decryption is initiated with whatever method is appropriate to the way the file is represented in the third file.

66. The method as recited in claim 64, wherein the second file is recreated from the third file after the file is decrypted.

67. The method as recited in claim 66, comprising the further step of running a virus scan program on the second file after it is recreated.

68. A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

 selecting an algorithm to use with the file from the plurality of algorithms;
selecting an encryption key with a key value;
generating a file identifier from the encryption key, an algorithm identifier associated
with the selected algorithm and a data identifier associated with the file;
adding the file identifier to the file;
inputting a decryption key with a decryption key value;
validating the decryption key value with the key value associated with the file identifier;
and
using the key value and the selected algorithm to decrypt the file;
wherein the file is located in a document or image repository.

69. A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;
selecting an encryption key with a key value;
generating a file identifier from the encryption key, an algorithm identifier associated
with the selected algorithm and a data identifier associated with the file;
adding the file identifier to the file;
using the key value and the selected algorithm to encrypt the file and generate an
encrypted file;
sending the encrypted file from a first person to a second person over the Internet in an e-
mail message;

inputting a decryption key with a decryption key value;
validating the decryption key value with the key value associated with the file identifier;

and

using the key value and the selected algorithm to decrypt the file.

70. The method as recited in claim 69, wherein the first person is the same as the second person.

71. A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;

selecting an encryption key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;

adding the file identifier to the file;

using the key value and the selected algorithm to encrypt the file and generate an encrypted file;

inputting a decryption key with a decryption key value;

validating the decryption key value with the key value associated with the file identifier;

and

using the key value and the selected algorithm to decrypt the file;

wherein a portion of the file identifier is encrypted before it is inserted into the file.

72. The method as recited in claim 71, comprising the further step of decryption a portion of the file identifier before the decryption key value is validated.

73. The method as recited in claim 72, wherein all of the file identifier is encrypted before the decryption key value is validated.

74. A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;

selecting an encryption key with a key value;

generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;

adding the file identifier to the file;

using the key value and the selected algorithm to encrypt the file and generate an encrypted file;

inputting a decryption key with a decryption key value;

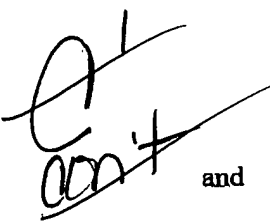
validating the decryption key value with the key value associated with the file identifier;

using the key value and the selected algorithm to decrypt the file;

invoking an option to initiate a virus scan program.

75. A method of encrypting and decrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;

 selecting an encryption key with a key value;
generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;
adding the file identifier to the file;
running a virus scan program on the file before it is encrypted;
using the key value and the selected algorithm to encrypt the file and generate an encrypted file;
inputting a decryption key with a decryption key value;
validating the decryption key value with the key value associated with the file identifier;
and
using the key value and the algorithm to decrypt the file;
wherein a portion of the file identifier is encrypted before it is inserted into the file.

76. A method of encrypting a file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the file from the plurality of algorithms;
selecting an encryption key with a key value;
generating a file identifier from the encryption key, an algorithm identifier associated with the selected algorithm and a data identifier associated with the file;
adding the file identifier to the file; and
uniquely identifying the encrypted file with an encrypted file header.

77. A method of decrypting an encrypted file with one of a plurality of algorithms, comprising the steps of:

selecting an algorithm to use with the encrypted file from the plurality of algorithms;
inputting an decryption key with a decryption key value;
validating the decryption key value with the key value associated with a file identifier that
was added to a file during an encryption process that created the encrypted file;
using the key value and the selected algorithm to decrypt the file;
testing the encrypted data identifier that is used to uniquely identify the encrypted file
during the encryption process by regenerating the encrypted data identifier and ascertaining that
they are the same.

78. A method of encrypting and decrypting a file with one of a plurality of algorithms, the method
comprising the steps of

selecting an algorithm to use with the file from the plurality of algorithms
selecting an encryption key with a key value
generating a file identifier from the encryption key, an algorithm identifier associated
with the selected algorithm and a data identifier associated with the file
adding the file identifier to the file
using the key value and the selected algorithm to encrypt the file and generate an
encrypted file
sending the encrypted file from a first person to a second person in an e-mail message.

79. A method of encrypting and decrypting a file with one of a plurality of algorithms, the method
comprising the steps of:

at
cont

receiving an encrypted file from a first person by a second person in an e-mail message

extracting a file identifier from the file

inputting a decryption key with a decryption key value

validating the decryption key value with a key value associated with the file identifier

using the key value and the selected algorithm to decrypt the file.
